Cooley

The DOJ's Bulk Sensitive Personal Data Rule's Imminent Relevance to Life Sciences Companies

April 2, 2025

A new US Department of Justice (DOJ) rule on "Preventing Access to US Sensitive Personal Data and Government-Related Data by Countries of Concern (including China) or Covered Persons" (rule) prohibits and restricts certain covered data transactions that result in the transfer or access to bulk US sensitive personal data by countries of concern or covered persons. The rule will take effect **April 8, 2025**.

Initial considerations for life sciences companies

Potentially relevant bulk thresholds

To determine whether data transactions trigger the "bulk" thresholds, the rule aggregates transactions over the preceding 12 months to determine the number of US persons' data implicated. In other words, it is a rolling assessment of whether a particular transaction crosses the relevant bulk thresholds. Different categories of sensitive personal data are associated with different bulk thresholds. Unlike with privacy-focused laws, the thresholds apply regardless of whether the data is anonymized, key-coded, pseudonymized, de-identified or encrypted, which presents significant challenges for life sciences companies. Of particular relevance for life sciences companies are the following:

Sensitive personal data category	Bulk threshold
Human genomic data (data representing the nucleic acid sequences that constitute the entire set or a subset of the genetic instructions found in a human cell) and/or **biospecimen data** (any quantity of tissue, blood, urine or other human-derived material from which human genomic data could be derived)	More than 100 US persons
Human 'omic data other than genomic data (e.g., human epigenomic data, human proteomic data and human transcriptomic data)	More than 1,000 US persons
Personal health data (health information that indicates, reveals or describes the past, present or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present or future payment for the provision of healthcare to an individual)	More than 10,000 US persons

Countries of concern or covered persons

The rule prohibits or restricts bulk sensitive personal data transactions with countries of concern or covered persons. The rule, while providing for future executive branch flexibility, defines countries of concern to include:

- The People's Republic of China (including Hong Kong and Macau)
- The Republic of Cuba
- The Islamic Republic of Iran
- The Democratic People's Republic of North Korea
- The Russian Federation
- The Bolivarian Republic of Venezuela

The rule creates four general categories of covered persons:

- Foreign entities that are 50% or more owned (directly or indirectly) by a country of concern, organized under the laws of a country of concern or have their principal place of business in a country of concern (including, potentially, a foreign subsidiary of a US company).
- Foreign entities that are 50% or more owned (directly or indirectly) by a covered person.
- Foreign employees or contractors of countries of concern, or of entities that are covered persons.
- Foreign individuals primarily resident in countries of concern.

The rule's impacts

Given the rule's breadth, its departure from existing US data privacy-focused laws, and significant civil and criminal fines and penalties, life sciences companies potentially within the rule's scope should consider how to minimize risks associated with "prohibited" and "restricted" transactions.

Prohibited transactions

In relation to bulk US sensitive personal data, the rule generally prohibits a few types of transactions that may result in foreign access to bulk US sensitive personal data.

- **Data brokerage transactions**: The rule prohibits "data brokerage" transactions, which include not only transactions that would typically be thought of as "data brokerage," i.e., the sale, in exchange for money, of data that was not collected directly from the individual to whom the data relates, but also any other transactions (excluding an employment agreement, investment agreement or a vendor agreement) involving the sale, licensing or similar commercial transactions of bulk sensitive personal data with countries of concern or covered persons.
    - To avoid circumvention of this requirement, the rule provides that data brokerage transactions with any other foreign person (i.e., not a covered person) must include a contractual provision requiring the foreign person to refrain from subsequent data brokerage transactions with countries of concern or covered persons.
- **Human 'omic data and human biospecimen transactions**: The rule prohibits covered data transactions with a country of concern or covered person that involve access by that country of concern or covered person to bulk US sensitive personal data where such sensitive personal data involves human 'omic or human biospecimens from which bulk human 'omic data could be derived. This second prohibition, absent the potentially relevant exemptions, could likely significantly impact life sciences companies given the low thresholds for human genomic data or human biospecimens to qualify as "bulk" and the broad definition of "access" under the rule. This prohibition has particular relevance for life sciences companies looking for investments from, or to use vendors or employees in, countries of concern or those who may qualify as covered persons.

Restricted transactions

The rule imposes restrictions on (but does not prohibit) covered data transactions involving certain vendor agreements, employment agreements or investment agreements with a country of concern or covered person, unless they involve bulk human 'omic data or human biospecimens from which such data could be derived.

The rule permits restricted transactions only if the US person complies with Cybersecurity and Infrastructure Security Agency (CISA) security requirements (effective October 6, 2025) and otherwise maintains a data compliance program that, in relevant part, establishes:

- Risk-based procedures for data flows.
- Risk-based procedures for vendor identity verification.
- An annual certification process of its data compliance program.
- An annual certification process of its data security program.

Potential exemptions for life sciences data transactions

In its background on the rule, the DOJ said it intends to address concerns about the rule's effects on drug development and biomedical innovation. To that end, the rule exempts certain data transactions from its prohibitions and restrictions, including

several exemptions potentially relevant to life sciences companies. These exemptions include:

- **Clinical and surveillance exemption**. Data transactions incident to and part of clinical investigations regulated by the FDA, or clinical investigations that support applications to the FDA for research and marketing permits (this includes post-marketing surveillance data, including pharmacovigilance and post-marketing studies for already approved therapies), provided that the clinical data is de-identified or pseudonymized in accordance with applicable FDA regulations.
- **Regulatory approval exemption**. Data transactions that involve "regulatory approval data," which are necessary to obtain or maintain regulatory approval to research or market a pharmaceutical product or medical device, provided that such data is de-identified or pseudonymized in accordance with applicable FDA regulations and is required to be submitted to a regulatory entity.
- **Federally funded research exemption**. Data transactions conducted pursuant to a US grant, contract or other agreement.

The breadth of these exemptions remains to be determined as adjudicatory bodies have yet to publicly interpret the rule's provisions.

Implications for life sciences transactions

The rule could apply to a variety of transactions involving life sciences companies. Below are just a few examples of scenarios in which life sciences companies (and their data transactions) could be within the rule's scope, and may or may not fall within the rule's exceptions:

- License or collaboration agreements between US entities and covered persons during which one of the parties conducts clinical trials in the United States and wants to transfer clinical data and/or biospecimens to a country of concern or covered person.
- M&A deals involving covered persons where one or more of the parties conducted clinical trials in the US.
- Vendor agreements (such as those with contract research organizations, contract manufacturing organizations or data-hosting providers) and employment agreements in which US sensitive personal data is shared with a country of concern or covered person.
- Intra-company sensitive personal data transactions.
- Investment agreements with investors who are in a country of concern or are otherwise covered persons.

What should life sciences companies do next?

Given the rule will soon take effect, life sciences companies should evaluate their exposure to the rule, take advantage of potential rule exemptions and, as appropriate, implement compliance strategies to address their obligations under the rule.

- **Determine whether you process bulk US sensitive data**. Evaluate whether the relevant data that you process (collect, transfer or receive) falls within the rule's scope.
- **Identify potential covered data transactions**. Undertake a review of any data brokerage, vendor, employment and investment agreements to determine whether the rule may apply to such transactions.
- **Know your company's data flows and conduct recipient diligence**. Know to whom and for what purposes you will transfer data/biospecimens and whether the recipient will engage in any further transfers. Conduct "know-your-recipient" diligence to assess whether they fall within the scope of the rule's definitions of countries of concern or covered persons.
- **Implement compliance strategies**. Update policies to identify potentially covered data transactions as part of the diligence process and implement and maintain:
    - Appropriate contractual protections on data transactions (aligned with good general data hygiene practices).
    - Internal policies, procedures and measures designed to limit access to data (particularly if personnel are in countries of

concern or are otherwise covered persons).

- Appropriate security measures for the sensitive personal data.

Key Contacts

Michael Egan Washington, DC	megan@cooley.com +1 202 776 2249
Daniel Grooms Washington, DC	dgrooms@cooley.com +1 202 776 2042
Alan W. Tamarelli New York	atamarelli@cooley.com +1 212 479 6470
Andrew Epstein Seattle	aepstein@cooley.com +1 206 452 8747
Carlton Forbes	cforbes@cooley.com +1 202 776 2117
Navya Dasari New York	ndasari@cooley.com +1 212 479 6952
Richard Koch Washington, DC	rkoch@cooley.com +1 202 776 2323